WHITE PAPER – Network Time Protocol (NTP)

Architecture, best practices and production operations

RDEM Systems – Systems and critical infrastructure expertise

January 2026

Introduction

NTP (Network Time Protocol) is a foundational component of modern IT infrastructure. Defined by RFC 5905, NTP synchronizes computer system clocks with millisecond precision over the Internet, and microsecond precision on local networks.

Reliable time synchronization is critical for:

- **Security**: TLS/SSL certificates, Kerberos authentication, TOTP tokens
- **Logging**: Event correlation across distributed systems
- **Compliance**: PCI-DSS, HIPAA, SOX requirements for audit timestamps
- **Applications**: Distributed databases, financial transactions, schedulers

A time drift of just a few seconds can cause authentication failures, log inconsistencies, and even data corruption in distributed systems.

Understanding NTP Strata

NTP uses a hierarchical system called **strata** (stratum) to organize time sources:

Stratum	Description	Typical Accuracy
0	Reference clocks (GPS, atomic clocks, DCF77)	< 1 µs
1	Servers directly connected to stratum 0	< 10 µs
2	Servers synchronized to stratum 1	< 100 µs
3-15	Cascading servers (each level adds latency)	1-100 ms
16	Unsynchronized (invalid)	-

Recommendation: For production use, use stratum 2 or 3 servers. Stratum 1 servers are typically reserved for NTP Pool operators or large organizations.

Why at least 3 NTP servers?

The number of NTP servers configured is critical for reliability:

- **1 server**: Single point of failure. No way to detect if the server drifts.
- **2 servers**: If they disagree, impossible to determine which is correct.
- **3 servers**: Quorum possible. If one server drifts, the other two can identify and exclude it (NTP selection algorithm).
- **4 servers**: Risk of 2/2 split in case of disagreement, reducing reliability.
- **5 servers**: Optimal configuration for critical environments.

General rule: Use an **odd** number of servers (3 or 5) to enable reliable consensus.

Recommended NTP Pools

RDEM Systems Infrastructure (recommended)

RDEM Systems operates a high-availability **Stratum 2** NTP infrastructure, hosted in France and contributing to the global NTP Pool Project (AS206014).

Server	Description
`pool-ntp.rdem-systems.com`	Global pool (11 Stratum 2 servers)
`pa3.pool-ntp.rdem-systems.com`	PA3 datacenter pool
`pa4.pool-ntp.rdem-systems.com`	PA4 datacenter pool
`pa5.pool-ntp.rdem-systems.com`	PA5 datacenter pool

Benefits: 24/7 monitored infrastructure, sub-millisecond accuracy, European hosting (GDPR), verifiable contribution: https://www.ntppool.org/a/rdem-systems

Alternatives: NTP Pool Project National Pools

As fallback, use national pools from pool.ntp.org. Each country has multiple servers accessible via prefixes 0, 1, 2 (e.g., `0.us.pool.ntp.org`).

USA	UK	Germany
`0.us.pool.ntp.org`	`0.uk.pool.ntp.org`	`0.de.pool.ntp.org`
`1.us.pool.ntp.org`	`1.uk.pool.ntp.org`	`1.de.pool.ntp.org`
`2.us.pool.ntp.org`	`2.uk.pool.ntp.org`	`2.de.pool.ntp.org`

Other countries available: `fr`, `ca`, `au`, `ch`, `be`, etc.

Continental pools: `europe.pool.ntp.org` | `north-america.pool.ntp.org` | `pool.ntp.org`

Windows Configuration (W32Time)

Check current status

```
w32tm /query /status
w32tm /query /configuration
w32tm /query /peers
```

Recommended configuration (RDEM Systems)

Run in **Administrator PowerShell**:

```
net stop w32time

$NTP = "pa3.pool-ntp.rdem-systems.com,0x1 " +
       "pa4.pool-ntp.rdem-systems.com,0x1 " +
       "pa5.pool-ntp.rdem-systems.com,0x1"

w32tm /config `
      /syncfromflags:manual `
      /reliable:YES `
      /update `
      /manualpeerlist:"$NTP"

net start w32time
w32tm /resync /force
```

Alternative with national pools (fallback)

```
$NTP = "0.us.pool.ntp.org,0x1 " +
       "1.us.pool.ntp.org,0x1 " +
       "2.us.pool.ntp.org,0x1"

w32tm /config /syncfromflags:manual /reliable:YES `
      /update /manualpeerlist:"$NTP"
```

Configuration flags

Flag	Description
0x1	Use as source
0x2	Use as fallback only
0x8	Use client mode (recommended)

Active Directory

Only the **PDC Emulator** should sync with external sources:

```
# PDC Emulator: see configuration above

# Other DCs (domain hierarchy)
w32tm /config /syncfromflags:domhier /update
```

Linux Configuration

Identify active service

```
timedatectl
systemctl status chronyd ntpd systemd-timesyncd
```

Chrony (recommended)

Chrony is the recommended NTP client for modern Linux distributions (RHEL 8+, Ubuntu 20.04+).

Installation

```
# Debian/Ubuntu
sudo apt install chrony

# RHEL/CentOS/Rocky/Alma
sudo dnf install chrony
```

Modern configuration (sources.d)

Create `/etc/chrony/sources.d/rdem-systems.sources`:

```
cat << 'EOF' | sudo tee /etc/chrony/sources.d/rdem-systems.sources
server pa3.pool-ntp.rdem-systems.com iburst
server pa4.pool-ntp.rdem-systems.com iburst
server pa5.pool-ntp.rdem-systems.com iburst
EOF

sudo chronyc reload sources
```

Classic configuration (/etc/chrony/chrony.conf)

```
# RDEM Systems servers
server pa3.pool-ntp.rdem-systems.com iburst
server pa4.pool-ntp.rdem-systems.com iburst
server pa5.pool-ntp.rdem-systems.com iburst

# Fallback
pool 0.us.pool.ntp.org iburst

driftfile /var/lib/chrony/drift
makestep 1.0 3
logdir /var/log/chrony
```

Useful commands

```
chronyc tracking        # Synchronization status
chronyc sources -v      # List sources
chronyc sourcestats     # Statistics
sudo chronyc makestep   # Force immediate correction
```

systemd-timesyncd (simple)

Configuration `/etc/systemd/timesyncd.conf`:

```
[Time]
NTP=pool-ntp.rdem-systems.com
FallbackNTP=0.us.pool.ntp.org 1.us.pool.ntp.org
```

Activation:

```
sudo systemctl enable --now systemd-timesyncd
timedatectl timesync-status
```

ntpd (legacy)

Configuration `/etc/ntp.conf`:

```
server pa3.pool-ntp.rdem-systems.com iburst
server pa4.pool-ntp.rdem-systems.com iburst
server pa5.pool-ntp.rdem-systems.com iburst
server 0.us.pool.ntp.org iburst

driftfile /var/lib/ntp/drift
restrict default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict ::1
```

Server vs Peer

Server (directive `server` or `pool`)

- Trusted external source
- Client → server relationship
- Used for public sources

Peer (directive `peer`)

- Peer at the same trust level
- Bidirectional relationship
- Used for synchronization between internal servers

```
Internet (pool.ntp.org)
        |
        v
   [NTP Server 1] <--peer--> [NTP Server 2]
        |                          |
        v                          v
   [Clients]                  [Clients]
```

Virtualized Environments

The Problem

VMs can receive time from two conflicting sources:

1. **Hypervisor** (VMware Tools, Hyper-V, QEMU Guest Agent)
2. **NTP** (system configuration)

Recommendation

Disable hypervisor time synchronization and use NTP only.

Hypervisor	Command
VMware	`vmware-toolbox-cmd timesync disable`
Hyper-V	`Disable-VMIntegrationService -VMName "VM" -Name "Time Synchronization"`
KVM/QEMU	Remove `kvmclock` or use `clocksource=tsc` kernel parameter

Exception: For VMs frequently suspended/resumed → keep hypervisor sync for large corrections.

NTP Security

Risks

- **DDoS amplification**: NTP can be exploited for reflection attacks
- **Time manipulation**: Attacker controlling time can invalidate certificates, bypass time-based protections

Best Practices

Firewall (client only)

```
iptables -A OUTPUT -p udp --dport 123 -j ACCEPT
iptables -A INPUT -p udp --sport 123 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp --dport 123 -j DROP
```

Chrony (disable remote access)

```
# /etc/chrony/chrony.conf
cmdport 0
bindcmdaddress 127.0.0.1
bindcmdaddress ::1
```

Multiple sources

Always configure **at least 4 sources** to detect malicious servers (Byzantine fault tolerance: 3f+1 servers to tolerate f compromised servers).

Troubleshooting

Symptom	Probable Cause	Solution
“No server suitable”	Firewall blocking UDP 123	Check iptables/firewalld
Large offset	First boot	`chronyc makestep`
Reach = 0	Server unreachable	Check DNS and connectivity
Stratum 16	Not synchronized	Check source configuration

```
ntpdate -q pool.ntp.org      # Test connectivity
dig +short 0.us.pool.ntp.org # Test DNS
nc -vzu pool.ntp.org 123     # Test UDP 123
```

References

- RFC 5905 – Network Time Protocol Version 4
- NTP Pool Project: https://www.ntppool.org
- Chrony Documentation: https://chrony.tuxfamily.org/documentation.html
- Microsoft W32Time: https://docs.microsoft.com/windows-server/networking/windows-time-service/

RDEM Systems – Systems and critical infrastructure expertise

- Contact: ntp@rdem-systems.com
- Website: https://ntp.rdem-systems.com
- NTP Pool contribution: https://www.ntppool.org/a/rdem-systems (AS206014)

NTP audit, architecture design and advanced support available on request.